

Exhibit 1

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION**

HEADWATER RESEARCH LLC

Plaintiff,

v.

SAMSUNG ELECTRONICS CO., LTD.,
SAMSUNG ELECTRONICS AMERICA, INC.

Defendants.

Case No. 2:23-CV-00103-JRG-RSP

**REBUTTAL EXPERT REPORT OF ERIK DE LA IGLESIA
REGARDING VALIDITY**



Date: October 14, 2024

Erik de la Iglesia

TABLE OF CONTENTS

I.	INTRODUCTION	1
A.	Retention	1
B.	Qualifications	2
C.	Materials Considered	4
D.	Legal Principles	5
E.	Claim Construction	11
F.	Level of Ordinary Skill	12
G.	Technology Background	12
1.	A Brief History of Networks and Network Communications	12
2.	The Rise in Smartphone Adoption: Network Congestion and Failures	18
3.	“Pull”-Model Network Communications	20
4.	“Push”-Model Network Communications	21
H.	General Comments on the Foster Report	25
I.	Rebuttal to Dr. Foster’s “Overview of the Prior Art”	26
1.	GTalkService	26
2.	Wireless Application Protocol	31
J.	Patent Background	32
1.	Summary of the ’117 Patent	32
2.	Summary of the ’733 Patent	33
3.	Summary of the ’192 Patent	33
II.	SUMMARY OF OPINIONS	34
III.	REBUTTAL TO DR. FOSTER’S OPINIONS ON THE ’117 PATENT	35
A.	GTalkService Alone or in Combination Does Not Anticipate or Render Obvious the Asserted Claims	35
1.	Claim 1[c]: “the network message server configured to receive, from each of a plurality of network application servers, multiple requests to transmit application data, each such request indicating a corresponding one of the mobile end-user devices and one of a plurality of applications”	36
2.	Claim 1[d] and 1[e]: “the network message server to generate corresponding Internet data messages based on the requests, each such message containing at least one application identifier for an indicated application and application data corresponding to one of the requests” Claim 1[e]: “the network message server to transmit each of the generated Internet data messages to the device messaging agent located on the device indicated in the corresponding request, using the	

corresponding secure Internet data connection for the device indicated in the corresponding request”	48
3. Claim 1[g]: “to, for each received message, map the application identifier in the message to a software process corresponding to the application identifier, and forward the application data in the message to the software process via a secure interprocess communication service.”	58
4. Claim 2: “The network system of claim 1, the network message server further to collect and buffer multiple requests to transmit application data to a particular one of the devices.”	72
5. Claim 4: “The network system of claim 1, the network message server further to encrypt the secure Internet data messages, the device messaging agents further to decrypt each received message to obtain the corresponding application identifier and application data.”	73
6. Claim 6: “The network system of claim 1, wherein the device messaging agent executes in a secure execution environment on at least one of the devices, and at least one of the applications executes outside of the secure execution environment on that device.”	74
7. Claim 10: “The network system of claim 1, wherein at least one of the secure Internet data messages comprises multiple identifier/data pairs.”	75
8. Claim 12: “The network system of claim 1, the device messaging agent on at least one of the devices further to initiate the secure connection to the network message server.”	75
9. Claim 13: “The network system of claim 1, at least one of the devices having a network stack in communication with the device messaging agent, wherein the secure connection between the network message server and that device is terminated within the network stack.”	75
10. Claim 16: “The network system of claim 2, wherein the network message server transmits the collected and buffered requests to the particular device upon the occurrence of a transmission trigger.”	76
11. Claim 17: “The network system of claim 16, wherein the transmission trigger is the expiration of a periodic timer.”	77
12. Claim 18: “The network system of claim 16, wherein the transmission trigger is the receipt of a transmission from the device messaging agent of the particular device.”	78
B. Lee Alone or in Combination Does Not Render Obvious the Asserted Claims	79
1. Claim 1[d]: “the network message server to generate corresponding Internet data messages based on the requests, each such message containing at least one application identifier for an indicated application and application data corresponding to one of the requests.”	79
2. Claim 1[g]: [each device messaging agent, when executing,] to, for each received message, map the application identifier in the message to a software process	

corresponding to the application identifier, and forward the application data in the message to the software process via a secure interprocess communication service.	81
3. Claim 2	86
4. Claim 4	86
5. Claim 6 – Dr. Foster fails to explain how “at least one of the applications executes outside of the secure execution environment on that device,” because in his proposed combination he alleges that each application would within a secure execution environment on the device.	86
6. Claim 10	87
7. Claim 12 – Dr. Foster does not establish the obviousness of “the device messaging agent on at least one of the devices further to initiate the secure connection to the network message server.”	88
8. Claim 13	88
9. Claim 16	88
10. Claim 17 – “The network system of claim 16, wherein the transmission trigger is the expiration of a periodic timer.”	89
11. Claim 18	90
C. OpenWave Mobile Access Gateway Alone or in Combination Does Not Render Obvious the Asserted Claims	90
1. Claim 1[a]: “a plurality of device messaging agents, each executable on a respective one of a plurality of mobile end-user devices configured to exchange Internet data via a data connection to a wireless network; and”	90
2. Claim 1[c]: “the network message server configured to receive, from each of a plurality of network application servers, multiple requests to transmit application data, each such request indicating a corresponding one of the mobile end-user devices and one of a plurality of applications,”	100
3. Claim 1[d]: “the network message server to generate corresponding Internet data messages based on the requests, each such message containing at least one application identifier for an indicated application and application data corresponding to one of the requests, and”	115
4. Claim 1[e]: “the network message server to transmit each of the generated Internet data messages to the device messaging agent located on the device indicated in the corresponding request, using the corresponding secure Internet data connection for the device indicated in the corresponding request;”	120
5. Claim 1[f]: “each device messaging agent, when executing, to receive the Internet data messages from the secure Internet data connection corresponding to the device executing the device messaging agent, and”	125
6. Claim 1[g]: “to, for each received message, map the application identifier in the message to a software process corresponding to the application identifier, and	

forward the application data in the message to the software process via a secure interprocess communication service.”	125
7. Claim 2: “The network system of claim 1, the network message server further to collect and buffer multiple requests to transmit application data to a particular one of the devices.”	135
8. Claim 4: “The network system of claim 1, the network message server further to encrypt the secure Internet data messages, the device messaging agents further to decrypt each received message to obtain the corresponding application identifier and application data.”	135
9. Claim 6: “The network system of claim 1, wherein the device messaging agent executes in a secure execution environment on at least one of the devices, and at least one of the applications executes outside of the secure execution environment on that device.”	136
10. Claim 10: “The network system of claim 1, wherein at least one of the secure Internet data messages comprises multiple identifier/data pairs.”	137
11. Claim 12: “The network system of claim 1, the device messaging agent on at least one of the devices further to initiate the secure connection to the network message server.”	137
12. Claim 13: “The network system of claim 1, at least one of the devices having a network stack in communication with the device messaging agent, wherein the secure connection between the network message server and that device is terminated within the network stack.”	137
13. Claim 16: “The network system of claim 2, wherein the network message server transmits the collected and buffered requests to the particular device upon the occurrence of a transmission trigger.”	138
14. Claim 17: “The network system of claim 16, wherein the transmission trigger is the expiration of a periodic timer.”	138
15. Claim 18: “The network system of claim 16, wherein the transmission trigger is the receipt of a transmission from the device messaging agent of the particular device.”	138
IV. REBUTTAL TO DR. FOSTER’S OPINIONS ON THE ’733 PATENT	138
A. GTalkService Alone or in Combination Does Not Anticipate or Render Obvious the Asserted Claims	138
1. Claim 1[b]: “a plurality of device agents communicatively coupled to the service control device link agent through an agent communication bus, each of the plurality of device agents identifiable by an associated device agent identifier; and”	139
2. Claim 1[e]: “using the encryption key, obtain a decrypted agent message, the decrypted agent message comprising a particular agent identifier and message content for delivery to a particular device agent of the plurality of device agents, the particular agent identifier identifying the particular device agent, the message	

content from a particular server of a plurality of servers communicatively coupled to the service control server link element”	146
3. Claim 1[f]: “based on the particular agent identifier, deliver the message content to the particular device agent over the agent communication bus.”	149
4. Claim 3: “The end-user device recited in claim 1, wherein the message content comprises information associated with a service usage.”	150
5. Claim 7: “The end-user device recited in claim 1, wherein the message content comprises a service offer, an advertisement, or a transaction offer.”	151
6. Claim 8: “The end-user device recited in claim 1, wherein the message content comprises information from a third party configured to provide control of a service or a billing for a service.”	152
7. Claim 9: “The end-user device recited in claim 1, wherein the message content comprises an agent instruction, a setting value, an agent configuration, or a software update.”	153
8. Claim 13: “The end-user device recited in claim 1, wherein the service control device link agent is further configured to send a device message to the service control server link element over the service control link.”	154
9. Claim 19: “The end-user device recited in claim 1, further comprising a user interface, and wherein the particular device agent is configured to assist in presenting a notification through the user interface, the notification based on the message content.”	154
10. Claim 23: “The end-user device recited in claim 1, wherein the service control device link agent is further configured to send a device credential to the network system or receive the device credential from the network system during a service authorization sequence.”	155
11. Claim 30[b]: “using an encryption key shared between the service control device link agent and the network element, obtaining a decrypted agent message, the decrypted agent message comprising a particular agent identifier and message content for delivery to a particular device agent of a plurality of device agents on the end-user device, each of the plurality of device agents identifiable by an associated device agent identifier and communicatively coupled to the service control device link agent through an agent communication bus, the particular agent identifier identifying the particular device agent, the message content from a particular server of a plurality of servers communicatively coupled to the network element”	156
12. Claim 30[c]: “delivering the message content to the particular device agent over the agent communication bus based on the particular agent identifier.”	156
B. Motorola E815 in view of Ogawa Does Not Render Obvious the Asserted Claims	157
1. Claim 1[b]: “a plurality of device agents communicatively coupled to the service control device link agent through an agent communication bus, each of the	

- plurality of device agents identifiable by an associated device agent identifier;
and”158
2. Claim 1[c]: “memory configured to store an encryption key, the encryption key shared between the service control device link agent and a service control server link element of the network system;”161
 3. Claim 1[d]: “wherein the service control device link agent is configured to: receive, over the service control link, an encrypted agent message from the service control server link element,”161
 4. Claim 1[e]: “[wherein the service control device link agent is configured to:] using the encryption key, obtain a decrypted agent message, the decrypted agent message comprising a particular agent identifier and message content for delivery to a particular device agent of the plurality of device agents, the particular agent identifier identifying the particular device agent, the message content from a particular server of a plurality of servers communicatively coupled to the service control server link element, and”162
 5. Claim 1[f]: “[wherein the service control device link agent is configured to:] based on the particular agent identifier, deliver the message content to the particular device agent over the agent communication bus.”164
 6. Claim 3: “The end-user device recited in claim 1, wherein the message content comprises information associated with a service usage.”165
 7. Claim 7: “The end-user device recited in claim 1, wherein the message content comprises a service offer, an advertisement, or a transaction offer.”165
 8. Claim 8: “The end-user device recited in claim 1, wherein the message content comprises information from a third party configured to provide control of a service or a billing for a service.”166
 9. Claim 9: “The end-user device recited in claim 1, wherein the message content comprises an agent instruction, a setting value, an agent configuration, or a software update.”167
 10. Claim 13: “The end-user device recited in claim 1, wherein the service control device link agent is further configured to send a device message to the service control server link element over the service control link.”167
 11. Claim 19: “The end-user device recited in claim 1, further comprising a user interface, and wherein the particular device agent is configured to assist in presenting a notification through the user interface, the notification based on the message content.”168
 12. Claim 23: “The end-user device recited in claim 1, wherein the service control device link agent is further configured to send a device credential to the network system or receive the device credential from the network system during a service authorization sequence.”169
 13. Claim 30[a]: “receiving, over a service control link, an encrypted agent message from a network element, the service control link secured by an encryption

protocol, the service control link supporting control-plane communications between a service control device link agent on the end-user device and the network element;”	169
14. Claim 30[b]: “using an encryption key shared between the service control device link agent and the network element, obtaining a decrypted agent message, the decrypted agent message comprising a particular agent identifier and message content for delivery to a particular device agent of a plurality of device agents on the end-user device, each of the plurality of device agents identifiable by an associated device agent identifier and communicatively coupled to the service control device link agent through an agent communication bus, the particular agent identifier identifying the particular device agent, the message content from a particular server of a plurality of servers communicatively coupled to the network element; and”	170
15. Claim 30[c]: “delivering the message content to the particular device agent over the agent communication bus based on the particular agent identifier.”	170
C. Microsoft Exchange ActiveSync Alone or in Combination Does Not Anticipate or Render Obvious the Asserted Claims	170
1. Claim 1[b]: “a plurality of device agents communicatively coupled to the service control device link agent through an agent communication bus, each of the plurality of device agents identifiable by an associated device agent identifier; and”	171
2. Claim 1[e]: [wherein the service control device link agent is configured to:] “using the encryption key, obtain a decrypted agent message, the decrypted agent message comprising a particular agent identifier and message content for delivery to a particular device agent of the plurality of device agents, the particular agent identifier identifying the particular device agent, the message content from a particular server of a plurality of servers communicatively coupled to the service control server link element”	173
3. Claim 1[f]: [wherein the service control device link agent is configured to:] “based on the particular agent identifier, deliver the message content to the particular device agent over the agent communication bus.”	177
4. Claim 3: “The end-user device recited in claim 1, wherein the message content comprises information associated with a service usage.”	179
5. Claim 7: “The end-user device recited in claim 1, wherein the message content comprises a service offer, an advertisement, or a transaction offer.”	179
6. Claim 8: “The end-user device recited in claim 1, wherein the message content comprises information from a third party configured to provide control of a service or a billing for a service.”	180
7. Claim 9: “The end-user device recited in claim 1, wherein the message content comprises an agent instruction, a setting value, an agent configuration, or a software update.”	180

8. Claim 13: “The end-user device recited in claim 1, wherein the service control device link agent is further configured to send a device message to the service control server link element over the service control link.”	181
9. Claim 19: “The end-user device recited in claim 1, further comprising a user interface, and wherein the particular device agent is configured to assist in presenting a notification through the user interface, the notification based on the message content.”	181
10. Claim 23: “The end-user device recited in claim 1, wherein the service control device link agent is further configured to send a device credential to the network system or receive the device credential from the network system during a service authorization sequence.”	182
11. Claim 30[b]	182
12. Claim 30[e]	182
V. REBUTTAL TO DR. FOSTER’S OPINIONS ON THE ’192 PATENT	182
A. GTalkService	182
1. Claim 1[b]: “an interface to a network to receive network element messages from a plurality of network elements, the received network element messages comprising respective message content and requests for delivery of the respective message content to respective wireless end-user devices, the respective message content including data for, and an identification of, a respective one of the authorized software components”	183
2. Claim 1[c]-1[e]: “a message buffer system including a memory and logic” Claim 1[d]: “the memory to buffer content from the received network element messages for which delivery is requested to a given one of the wireless end-user devices” Claim 1[e]: “the logic to determine when one of a plurality of message delivery triggers for the given one of the wireless end-user devices has occurred, wherein for at least some of the received network element messages, the receipt of such a message by the message buffer system is not a message delivery trigger, and for at least one of the message delivery triggers, the trigger is an occurrence of an asynchronous event with time-critical messaging needs”	190
1. Claim 5: “The message link server of claim 1, wherein the transport services stack is further to receive, over each of the respective secure message links, upload messages forwarded by the respective device link agents from at least a subset of the device software components, each of the upload messages identifying a corresponding one of the network elements to which the device respective software component has requested delivery, the network server system using the interface to a network to deliver content from the upload messages to the respective identified network elements.”	192
2. Claim 7: “The message link server of claim 1, the device messaging agent on at least one of the wireless end-user devices further to initiate the respective secure Internet data message link to the transport services stack.”	192

3. Claim 8: “The message link server of claim 1, further comprising a secure server to provide secure authorization signatures to the given one of the wireless end-user devices, the secure authorization signatures indicating the authorized software components that are allowed to receive data from secure message link messages via the message link server.”	192
4. Claim 9: “The message link server of claim 1, wherein one of the message delivery triggers is the expiration of a periodic timer.”	194
5. Claim 11: “The message link server of claim 1, wherein one of the message delivery triggers is the receipt of a transmission on the respective secure message link from the device link agent of the given one of the wireless end-user devices, or a response generated to a transmission received from that device link agent.”	195
B. OpenWave Mobile Access Gateway Alone or in Combination Does Not Render Obvious the Asserted Claims	195
1. Claim 1[a]: “a transport services stack to maintain a respective secure message link through an Internet network between the message link server and a respective device link agent on each of a plurality of wireless end-user devices, each of the wireless end-user devices comprising multiple software components authorized to receive and process data from secure message link messages received via a device link agent on that device;”	195
2. Claim 1[b]: “an interface to a network to receive network element messages from a plurality of network elements, the received network element messages comprising respective message content and requests for delivery of the respective message content to respective wireless end-user devices, the respective message content including data for, and an identification of, a respective one of the authorized software components; and”	212
3. Claim 1[e]: “the logic to determine when one of a plurality of message delivery triggers for the given one of the wireless end-user devices has occurred, wherein for at least some of the received network element messages, the receipt of such a message by the message buffer system is not a message delivery trigger, and for at least one of the message delivery triggers, the trigger is an occurrence of an asynchronous event with time-critical messaging needs, and”	218
4. Claim 1[f]: “upon determining that one of the message delivery triggers has occurred, the logic further to supply one or more messages comprising the buffered content to the transport services stack for delivery on the secure message link maintained between the transport services stack and a device link agent on the given one of the wireless end-user devices.”	219
5. Claim 5: “The message link server of claim 1, wherein the transport services stack is further to receive, over each of the respective secure message links, upload messages forwarded by the respective device link agents from at least a subset of the device software components, each of the upload messages identifying a corresponding one of the network elements to which the device respective software component has requested delivery, the network server system using the	

interface to a network to deliver content from the upload messages to the respective identified network elements.”	219
6. Claim 7: “The message link server of claim 1, the device messaging agent on at least one of the wireless end-user devices further to initiate the respective secure Internet data message link to the transport services stack.”	219
7. Claim 8: “The message link server of claim 1, further comprising a secure server to provide secure authorization signatures to the given one of the wireless end-user devices, the secure authorization signatures indicating the authorized software components that are allowed to receive data from secure message link messages via the message link server.”	220
8. Claim 9: “The message link server of claim 1, wherein one of the message delivery triggers is the expiration of a periodic timer.”	220
9. Claim 11: “The message link server of claim 1, wherein one of the message delivery triggers is the receipt of a transmission on the respective secure message link from the device link agent of the given one of the wireless end-user devices, or a response generated to a transmission received from that device link agent.”	221
C. Microsoft Exchange Server System Does Not Anticipate or Render Obvious the Asserted Claims	221
1. Claim 1[a]: “a transport services stack to maintain a respective secure message link through an Internet network between the message link server and a respective device link agent on each of a plurality of wireless end-user devices, each of the wireless end-user devices comprising multiple software components authorized to receive and process data from secure message link messages received via a device link agent on that device;”	222
2. Claim 1[b]: “an interface to a network to receive network element messages from a plurality of network elements, the received network element messages comprising respective message content and requests for delivery of the respective message content to respective wireless end-user devices, the respective message content including data for, and an identification of, a respective one of the authorized software components; and”	224
3. Claim 1[c]: “a message buffer system including a memory and logic,” Claim 1[d] “the memory to buffer content from the received network element messages for which delivery is requested to a given one of the wireless end-user devices,”	226
4. Claim 1[e]: “the logic to determine when one of a plurality of message delivery triggers for the given one of the wireless end-user devices has occurred, wherein for at least some of the received network element messages, the receipt of such a message by the message buffer system is not a message delivery trigger, and for at least one of the message delivery triggers, the trigger is an occurrence of an asynchronous event with time-critical messaging needs, and”	227
5. Claim 5: “The message link server of claim 1, wherein the transport services stack is further to receive, over each of the respective secure message links, upload messages forwarded by the respective device link agents from at least a subset of	

the device software components, each of the upload messages identifying a corresponding one of the network elements to which the device respective software component has requested delivery, the network server system using the interface to a network to deliver content from the upload messages to the respective identified network elements.”228

6. Claim 7: “The message link server of claim 1, the device messaging agent on at least one of the wireless end-user devices further to initiate the respective secure Internet data message link to the transport services stack.”228

7. Claim 8: “The message link server of claim 1, further comprising a secure server to provide secure authorization signatures to the given one of the wireless end-user devices, the secure authorization signatures indicating the authorized software components that are allowed to receive data from secure message link messages via the message link server.”228

8. Claim 9: “The message link server of claim 1, wherein one of the message delivery triggers is the expiration of a periodic timer.”229

9. Claim 11: “The message link server of claim 1, wherein one of the message delivery triggers is the receipt of a transmission on the respective secure message link from the device link agent of the given one of the wireless end-user devices, or a response generated to a transmission received from that device link agent.” .229

VI. VALIDITY UNDER 35 U.S.C. § 112229

 D. ’733 Patent Claims229

 E. ’117 Patent Claims232

 1. “application identifier” limitations233

 2. “secure interprocess communications” limitations237

VII. REBUTTAL TO DR. FOSTER’S OPINIONS ABOUT THE ASSERTED PATENTS BEING “WELL-UNDERSTOOD, ROUTINE, AND CONVENTIONAL”239

VIII. SECONDARY CONSIDERATIONS254

 A. Commercial Success and Industry Recognition255

 B. Long-Felt Need and Failures of Others259

IX. NON-INFRINGEMENT ALTERNATIVES267

X. CONCLUSION.....277

B. Lee Alone or in Combination Does Not Render Obvious the Asserted Claims

239. Dr. Foster references IPR2024-00003, as supposedly showing the obviousness of the '117 Patent. Dr. Foster says he “agree[s] with the analysis of the IPR petition and its supporting materials,” and says he “reproduce[s] some of that analysis below and adopt[s] it as [his] own opinions.” Foster Rpt. ¶ 552. However, what Dr. Foster neglects to acknowledge is that the Patent Trial and Appeal Board of the United States Patent and Trademark Office already considered and disagreed with the analysis in IPR2024-00003. *See* IPR2024-00003 at Paper No. 8.

240. Furthermore, there are numerous reasons why Lee alone or in combination with other references does not disclose or render obvious the asserted claims, as explained in further detail below.

241. Moreover, there is significant evidence of secondary considerations (e.g., commercial success, long-felt need, failures of others, praise, awards, industry recognition, copying) that further support my opinions that the asserted claims would not have been obvious to a POSITA, which are discussed below and hereby incorporated by reference.

1. ***Claim 1[d]: “the network message server to generate corresponding Internet data messages based on the requests, each such message containing at least one application identifier for an indicated application and application data corresponding to one of the requests.”***

242. Claim limitation 1[d] recites: “the network message server to generate corresponding Internet data messages based on the requests, each such message containing at least one application identifier for an indicated application and application data corresponding to one of the requests.”

243. Dr. Foster acknowledges that a requirement of this limitation is that “‘each’ message generated by the network message server [must] contain an ‘application identifier’ and ‘application data.’” Foster Rpt. ¶ 585. I disagree, however, that Lee teaches or renders obvious this requirement.

244. For example, Dr. Foster does not provide any express teaching from Lee that “each” message would include application data. Thus, there is no dispute that Lee does ***not*** actually teach

as much.

245. His only allegation that this requirement would have been obvious is that “a message with only an application identifier and no application data would be pointless.” Foster Rpt. ¶ 585. However, that assertion is, in my opinion, based on a misunderstanding of how the Lee system worked to “invoke” applications.

246. Specifically, Lee teaches “selectively invoke[ing] the application 260 corresponding to the associated application ID”—in other words, it tells the application to begin executing so that the application can itself retrieve the message data. Lee ¶[29]. “Invoking,” in the context of computer software processes, an application does not mean “forwarding data to the application,” but instead means *causing the application to execute*. By *selectively* invoking applications in this manner, it “reduc[es] a number of the applications resident in memory,” thereby reducing “power consumption.” *Id.*; see also *id.* FIG. 8 (showing the integrated push service agent “invok[ing] application corresponding to app_ID”).

247. Thus, Lee uses the application ID to inform applications that they should begin running. A POSITA would recognize that an application that receives an invocation request with no application ID pursuant to a push message could be programmed to contact its associated application server through a direct connection to retrieve any needed data from that server without the push client needing to act as an intermediary.

248. For example, an important use-case for such an implementation would be if the application server wanted to provide highly sensitive information to an application, and wished to use a *direct connection* to provide that information. Normally, this is difficult to accomplish, because the application might not be running on the device. But Lee’s application invocation process allows a way for the application server to request that the relevant application be *invoked*, and the application under such a scenario would be programmed to contact the application server. No application data would need to be transmitted along with the invocation message, because contacting the application server upon invocation would be part of the application’s programming.

249. One example of this implementation (which is consistent with Lee’s teachings) is

a scenario where a bank application server needs to transmit data securely to a user's banking application, but wants to do so over a direct connection. For instance, if the Chase banking network had an important security alert for the user, it could simply inform Lee's system to invoke the Chase banking application (without actually providing application data to the application); the banking app would then contact the Chase banking network server upon invocation, and the network server could securely inform the banking app of the security alert. This would avoid the need for complex security mechanisms, and would not involve the invocation message sent to the application including any application data.

2. ***Claim 1/g]: [each device messaging agent, when executing,] to, for each received message, map the application identifier in the message to a software process corresponding to the application identifier, and forward the application data in the message to the software process via a secure interprocess communication service.***

- a. No motivation to combine with Kalibjian.

250. Dr. Foster's proposed combination of Kalibjian, memory in the device is "divided into 'separate and distinct secure sections.'" Foster Rpt. ¶ 596. Under the proposed combination, each application would need to operate in a separate partition from other applications, such that no application could potentially have access to information intended for another application (or corrupt other applications). *See* Kalibjian ¶[0020] ("A secure operating system includes secure memory partitions or processing space that insures applications running in one partition 10A cannot gain access and corrupt applications running in another partition 210B."); Foster Rpt. ¶ 617 ("In the Lee-Kalibjian combination, the push client would have been incorporated into one of these secure sections, with applications incorporated into other secure sections....").

251. Dr. Foster provides two alleged motivations to do so. His first motivation is "to address 'security concerns' such as different applications running on the mobile terminal intercepting or interfering with messages exchanged between Lee's push service agent 250... and application 230." Foster Rpt. ¶ 597.

252. This motivation (avoiding intercepting or interfering with messages) fails because he does not allege that Lee's mobile device suffered from any such problem. (I note that neither